

MCI

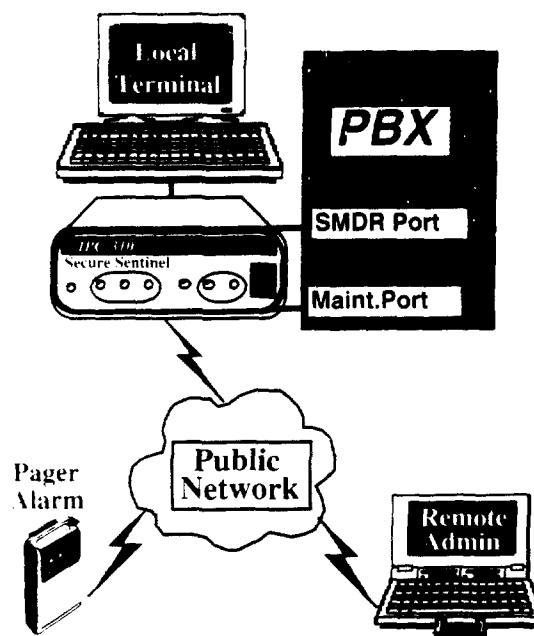
In Affiliation With

MicroFrame

No Additional Lines, Easy Installation and Initialization

Both the remote access maintenance port and SMDR port connect to the IPC-310, eliminating the cost of extra support lines and modems. Initialization is easily accomplished through a series of menu-driven prompts.

Any combination of available authentication technologies may be selected for maintenance port access. Up to 20 user-defined CDR control parameters are available for setting alarm criteria, including both percent deviation from normal profiles and number-of-events limitations in each parameter.



Technical Specifications

Basic Secure Sentinel® IPC-310 Platform

Authentication Models	Type
Callback:	Fixed/Variable Callback, Password Only
Direct Dial Token:	In-Line: TeleKEY, MagnaKEY, SofKEY Off-Line: PassKEY and Other Popular Tokens
Operating Characteristics	
Internal Modem:	2400 bps with MNP level 5 Error Correction ANI Compatible
Maximum Link Speed:	19.2 Kbps, Speed Matching between Ports
Digital Connections:	Host 1-RS-232/DB25S, Host 2-RS232/DB9S Aux Port-RS-232/DB25S
Analog Connections:	RJ11
Standard Display:	Red, Green, Yellow LED Indicators
Standard Power:	110/220/240 VAC, 50/60 Hz
Optional Power:	48V to 52V DC
Back-up Power:	Holdover Battery included
Standard Memory:	1MB Battery Supported Static RAM
Buffer memory:	Programmable
Temperature Range:	0-40 degrees Centigrade
Relative Humidity:	To 95%, non-condensing
Dimensions	5.75"x9.50"x2.75"

FOR INFORMATION

CALL 1(800)395-7450

MicroFrame, Inc.

21 Meridian Road

Edison, NJ 08820

MCI

In Affiliation With

MicroFrame

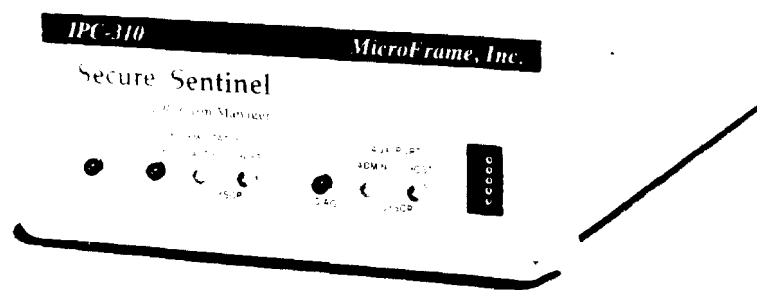
IPC-310 SECURE SENTINEL

Dual-port controller with internal modem provides continuous toll fraud loss control through real-time call-detail monitoring, maintenance port security, and alarm management.

The MicroFrame Secure Sentinel integrates the essential elements of a sound telephone fraud loss prevention program into a single solution. The Secure Sentinel connects to both the SMDR and the maintenance port of the PBX, securing the maintenance port against unauthorized access and detecting fraudulent activity by continuously monitoring call detail records. It provides prompt control action through alarms to PCs, pagers or FAX machines. If there is no response to the initial alarm within a pre-selected time, Secure Sentinel escalates alarms to higher authority and/or can automatically disable the abused facility.

MicroFrame has been a leader in programmable computer and data network security systems since 1982. Companies of all sizes rely on the Secure Sentinel as a key element in their fraud loss control program.

Installation and initialization is quick and easy. For more information, contact MicroFrame, Inc., at 1(800)395-7450.



Realize the Following Benefits

- Continuous monitoring and analysis of call-detail records to determine if activity exceeds predefined threshold levels
- Secured access to PBX maintenance ports using advanced caller authentication technologies
- All call activity captured and logged
- Intelligent "auto-learn" mode to establish CDR profiles
- Automatic alarm notification to PC, pager or FAX
- Escalation of alarms to higher level if no response within selected time frame
- Automatic shut-down capability if no response to alarms
- Special 20% discount on entire line of MicroFrame products for all MCI customers

MCI

In Affiliation With

Xiox

THE HACKER PREVENTER™

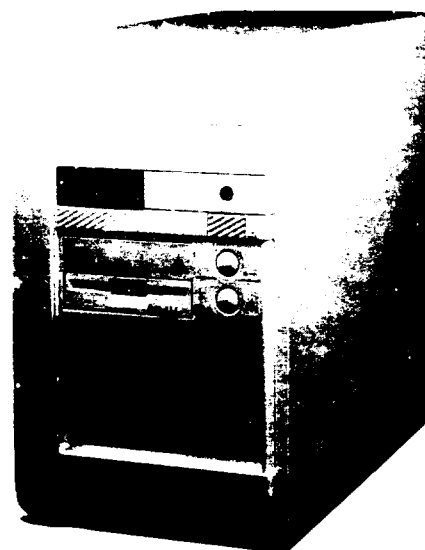
Advanced artificial intelligence provides continuous, high level security against fraudulent access to PBX.

The Xiox Hacker Preventer provides a unique, proactive approach to telecommunications fraud control. Using three lines of defense, it guards inbound access to PBX systems, blocking the efforts of even highly sophisticated hackers. This is achieved through a combination of user ID, password, and verbal authorization, making the probability of guessing a valid code one in a billion. Repeated access attempts and unusual call patterns are recognized and access is denied.

Drawing upon experience and expertise gained over more than a decade of providing PC-based call accounting and telecommunications security, Xiox offers a complete family of hardware and software for successfully blocking, tracking and trapping hackers and system abusers. In addition to the Hacker Preventer, the Fort Knox family includes the Hacker Deadbolt and the Hacker Tracker.

Realize The Following Benefits

- Three levels of inbound protection from telephone hackers
- Secure, monitored use of DISA-type features for traveling employees and telecommuters



- Automatic recognition of user-profile deviations and termination of fraudulent use
- On-demand printed reports for assistance with fraud analysis and usage research
- Secure access to remote maintenance ports, voice-mail systems and modem pools
- Full realization of cost savings inherent to remote access systems
- Special 20% discount on entire family of XIOX products to all MCI customers

Easy Installation and Custom Configuration

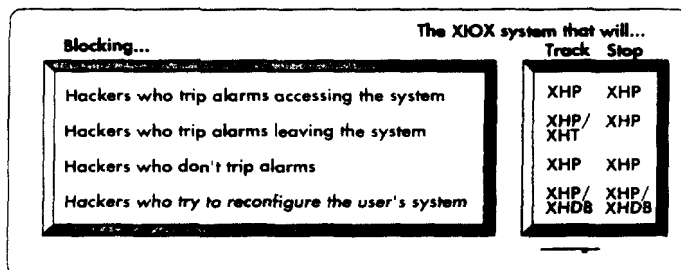
Within hours, the Xiox Hacker Preventer can be installed and configured to meet the precise security needs of your organization. The unit connects between one and sixteen extensions to your PBX and requires no special trunking or telecomm facilities. It can accommodate over 2,000 busy hour calls (depending on model) through the DIT feature. Configuration and maintenance can be accomplished either by secure telephone or by using the DOS-based configuration utility provided with the Hacker Preventer.

MCI

In Affiliation With

Xiox

- Stop inbound hackers...three levels of access protection include user ID and password, verbal password, and alarming.
- Stop outbound hackers...user IDs can be assigned to nine defined classes of service for specific destinations such as interoffice or certain area codes, or restricted from access to certain destinations such as international or any long distance calls.
- Stop hackers who don't trip alarms when leaving system...proprietary user profiling, automated accumulation of profiles, and artificial intelligence comparisons to profiles separate hackers from users.
- Stop hackers who try to reconfigure the user system...the remote maintenance port is protected by an array of password alternatives; a dial back modem capability and passwords in effect for limited periods such as one-time or 24-hour use.
- Track hackers...robust reporting capabilities include Authorized User, Call Detail, Active User IDs, and Daily Activity by User ID.



MATRIX KEY:

XHT= Xiox Hacker Tracker XHDB= Xiox Hacker Deadbolt

Trunks



IRISA™
Intelligent Restricted
Inward System Access

Telecommuters

Software
Defined Networks

FOR INFORMATION

CALL 1(800)685-8188

XIOX Corporation

577 Airport Blvd., Suite 700

Burlingame, CA 94010

Technical Specifications

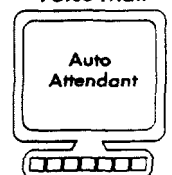
The Hacker Preventer™

Physical	Housing: Shelf or desk mounted enclosure H 13.5 in. W 7.5 in. D 16 in. Weight, exclusive of packing materials: 28 pounds.
Electrical	Mains power: 115/230 Vac. 50-60 Hz, 50 VA max. 25 VA typical.
Environment	Operating temperature 10-50 deg. C. Relative Humidity 10-95%
Telephone	RJ11 analog, FCC registration: EMC54S-15118-MD-E Reqv: 0.8B ULE10 1818.
Functional	User ID code length: 8 digits maximum, 1 digit minimum. Dialed number length: 28 digits maximum. Global Service Classes: 0 restricted 1&2 unrestricted User Service Classes: 0 restricted, 1-9 unrestricted.
Reports	Authorized User ID list, selectable by range of user code. Call detail report, last in-first out, 5000 call sliding window. Active User Report, selectable by range of user code. Daily Active User Report.

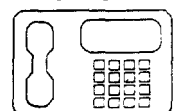
Modem Pool



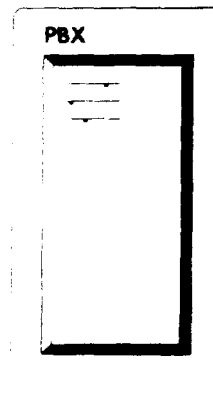
Voice Mail



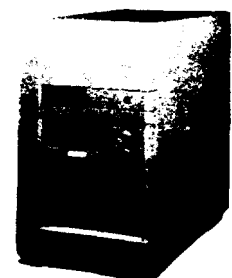
Stations



PBX



Remote
Maintenance Ports



MCI DETECTOR

Volume 1, Issue 1
Spring 1993

A publication
on the issues of
Telecommunications
Fraud Prevention

Welcome to the New MCI Detector

This is the first edition of the MCI Detect newsletter, DETECTOR. We have designed this publication to provide you with an overview of MCI's fraud prevention features, information on the latest fraudulent techniques, helpful hints on how to deal with fraud and feature stories on how we have helped customers.

A growing number of companies have been confronted with the toll fraud problem. While estimates vary, it is generally acknowledged that CPE-related fraud accounts for more than \$1 billion each year in losses. The possibility of being hacked is very real.

MCI has a long history of helping our customers deal with fraud problems including holding fraud prevention seminars, providing on-site consulting and supplying educational materials.

Now a new generation of anti-fraud measures have been developed to combat toll fraud. MCI Detect is a value-added service developed to "HELP YOU PUT THE FINGER ON FRAUD." It is a multi-faceted approach consisting of 4 key elements:



1. Customer Awareness & Education — Free to MCI Customers

- Exclusive, award winning, fraud awareness video, "Invisible Criminals"
- MCI DETECTOR, quarterly informative newsletter
- Manual on easily compromised CPE features and functions (available mid-1993)
- "Hands on" consulting



2. Analysis of Customer Traffic — Free to MCI Customers!

- Analysis of customer's MCI domestically originated 800 traffic and outbound international to select high-fraud countries

- Customer notification of potentially fraudulent usage
- Assistance in resolving fraudulent situations



3. CPE Add-on Equipment through Affiliates Program

- 20% discount on MicroFrame and Niox equipment for MCI customers
- Monitors any traffic routed through it; is not exclusive to the traffic of MCI or any other carrier
- Can be set to take corrective action without human intervention
- Has thresholds that can be tailored to individual business traffic patterns
- Monitors traffic on real time basis



4. Third-Party Insurance

- Coverage of all of customer's long distance traffic
- No MCI requirement for traffic volume commitment
- True insurance, not a service guarantee

For more information on how MCI Detect can help you put the finger on fraud speak with your MCI representative.

**MCI intercepts fraudulent
activity on Times Record in
Maine 1-800 service and
prevents thousands of
dollars in losses.**

hints

MCI has a long history of helping our customers with fraud problems.

DISA

Fraud Method(s)—DISA is designed to allow remote access to a PBX and then originate an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call-sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer." The "war dialer" dials telephone numbers randomly, generally 800 numbers, until a modem or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (auth codes). Codes are "frequently" but not always distributed to pirated voice mail systems and computer bulletin boards. The codes are usually distributed to a network of call-sell operators and may also be posted on bulletin boards and voice mail systems.

Fraud Solution(s)—There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin with auth codes should be made as long as possible. At the very least a factor of 10,000 should exist between the active codes. For example, if there are 10 users the code should be at least 5 digits long ($10 \times 10,000 = 100,000$ or 5 digits). Auth codes should be randomly scattered throughout the possible range but not easily defined (e.g. 1234 or 1111). Class of service restrictions should be applied to the auth codes. Only users with a truly legitimate need should be allowed International dialing through the DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show the number of times and minutes an auth code is used in a day. If possible, the dollar value of those calls should also be noted on the reports.

Voice Mail Boxes (VMB) As Bulletin Board

Fraud Method(s)—There are two types of VMB Systems fraud. The first type occurs when a hacker takes over a box and uses it to communicate with other hackers. This can be

expensive if access is gained to the VMB System via an 800 number. In this situation, a hacker typically backs out the box password and changes it along with the greeting.

Fraud Solution(s)—To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the phone. If telecom person can add, delete and change boxes via the phone, so can a hacker.
- Do not have active mail boxes that do not have an owner.
- Passwords should be at least 6 digits long.
- If possible, passwords should expire every 30-90 days.

Voice Mail Boxes (VMB) Garnering Dial Tone

Fraud Method(s)—The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a phone on the system. If the PBX is not set up properly the transfer can be made directly to dial tone. In other instances the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the tie line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBXs have Trunk Access Codes (TACs) or Facility Access Codes (FACs). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TACs or FACs.

Fraud Solution(s)—Steps to Prevent PBX Fraud:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4-digit extensions if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

Fraudulent Activity Discovered in Daily Analysis Report



MCI's Systems Integrity group recently came to the rescue of *The Times Record* in Brunswick,

Maine. Karen Curia, an SI Staff Investigator, noticed in the daily analysis report that an unusually high number of calls to *The Times Record's* 800 number were coming in from the 212 area code. Karen realized that this pattern was out of the norm for *The Times Record*, and that the 212 area code further indicated that fraudulent activity was occurring. A hacker most likely had just cracked an access code into *The Times Record* PBX and sold the code to an individual who sold long distance service for a fee from payphones,

**Brunswick,
Maine**

a.k.a., a "call-sell" operation. She immediately called *The Times Record* and advised them to contact their equipment vendor to secure their system.

As a result, the fraud-related losses were kept to less than \$500. Had this system of traffic analysis and prompt action by Karen not been in place, the loss could easily

have been in the tens of thousands of dollars. Phyllis A.

Thiboutot, Vice President and Treasurer of *The Times Record*, in commending

Karen said, "I especially would like to forward my heartfelt thanks

to Karen Curia for her work on our account; if it were not for

her, we would have

only discovered this problem

today. MCI Investigations has done

a superb job."

Congratulations Karen!

M C I D E T E C T I N A G T I O N

PRODUCT *News Update*

800 EXTENDED CALL COVERAGESM

Beginning April 5, 1993, basic MCI 800 ServiceSM and MCI VisionSM 800 Service will include calls from Hawaii, U.S. Virgin Islands and Puerto Rico. Previously, these areas were part of Extended Call Coverage. Basic coverage will now include these areas automatically. This 800 service enhancement gives you the opportunity to explore new markets outside the United States.

Although the U.S. Virgin Islands and Puerto Rico do not currently account for large amounts of CPE or card fraud, there is a degree of certainty that inbound 800 from Puerto Rico will be used to access and defraud customers' equipment.

We advise our customers to block outbound calls to the 809 area code (809 contains the Caribbean countries) as well as to countries not included in the North American Numbering Plan, unless they have business reasons to allow the calls. This precaution will prevent, or at least limit, the most expensive fraudulent calls, the international ones. Blocking outbound, however, does not prevent the hacker from dialing in to your equipment via your 800 number.

MCI 800 service can be tailored so that 800 calls can originate from the areas you specify. This is called Tailored Call Coverage.SM Using this capability, you can specify, by area code and exchange (also known as NPA & NXX), the areas you want to allow calls to originate from and the ones you do not. If, in the context of your business' requirements, you can prevent calls to your 800 number, from originating in a particular area, you have eliminated the possibility of fraud attacks via 800 access from that area.

As part of the changes to the areas included in Basic 800 coverage, MCI is waiving the Tailored Call Coverage (TCC) charge associated with blocking from April 1 until June 30. After June 30, there will be a \$150 install charge to block calls from these areas, and a \$110 change charge to include these areas (both one-time charges).

MCI is currently developing a list of NPA-NXX combinations from which significant amounts of fraud originate. This list will be made available to customers for consideration for possible exclusion from 800 coverage plans.

We hope that you have found the information contained in DETECTOR helpful in your efforts to prevent CPE-related fraud. Look for the next issue of DETECTOR in the third quarter of '93.

Are Thieves Using Your PBX?

Telephone fraud: an unfortunate tradition

by Jim Snyder

For as long as fees have been levied for telephone service, thieves have schemed to avoid paying these charges particularly for long-distance calling. Unfortunately, this thievery is not only flourishing, but the individuals involved are constantly developing more sophisticated techniques for perpetrating fraud.

Although telephone fraud existed prior to divestiture, it was less visible then because the associated costs were simply passed on to ratepayers. Following divestiture, however, the opportunities to make fraudulent long-distance calls multiplied.

The danger for the PBX owner is that the remote access authorization code will be compromised, enabling fraudulent calls to be originated through the PBX.

Long-distance carriers entering the market relied on five and six digit personal identification numbers to provide customers with access to their networks. As these codes were relatively easy for hackers to break, the companies relying on them were extremely vulnerable. To combat this type of fraud, long-distance service providers improved their defenses. In response, the thieves changed the targets and methods of their thievery.

Remote access fraud

Perhaps the most critical issue facing telecommunications users today is remote access fraud, typically accomplished through Private Branch Exchanges (PBXs) and electronic Voice Mail Boxes (VMBs).

Any business that employs a PBX or a VMB in its telecommunications system can incur hundreds of thousands of dollars in losses (in a few days) at the hands of those intent on stealing services.

PBXs at the heart of the problem

The heart of the problem lies with the capabilities of PBXs and similar equipment: not only is the PBX able to transfer calls to extensions and provide access to the public switched network, it generally has a number of other useful features, such as remote access capability.

Remote access capability permits a user to dial an 800 number or a 7 or 10 digit number assigned to the Remote Access Unit (RAU) or the Direct Inward System Access (DISA) feature of a PBX, to remotely enter an authorization code through the telephone touch tone pad, and to obtain a dial tone. Then, if no egress restrictions are in place in the PBX, a call to any other telephone in the world is generated.

Compromised codes

The danger for the PBX owner is that the remote access authorization code will be compromised, enabling fraudulent calls to be originated through the PBX. Typically, the criminal who has gained possession of a remote access authorization code

number will make a "free" inbound call to the PBX through the use of an 800 or a local number assigned to the customer's PBX, enter the compromised authorization code, and then dial the desired terminating number.

Once a PBX code has been compromised, it will be sold, then resold by each successive buyer again and again for as long as the code remains active. These codes are also used for "call-sell" operations in which long distance phone calls are "sold" to the public at pay phones and other locations.

The methods that are deployed against PBXs are limited only by the ingenuity of the criminals seeking to penetrate them.

How hackers invade PBXs

The methods that are deployed against PBXs are limited only by the ingenuity of the criminals seeking to penetrate them. For example, if the lines are automatically answered by a call sequencer, which routes incoming calls, the PBX is at risk. A "hacker" can program his computer to generate calls to an 800 or a local number and learn the security codes resident in the PBX during the time that the call is on hold waiting to be answered. A computer isn't necessary, however, to identify a valid security code. Simple security codes are often discovered by hand.

Obscene calls signal fraud

Receiving numerous wrong or obscene phone calls could indicate another variety of PBX fraud. The caller may be taking advantage of a design flaw in

PBX Fraud (continued)

older PBXs that returns a dial tone to the caller if the called party hangs up first. VMBs are also targets of this type of fraud since some systems provide a dial tone to the caller.

Owner is responsible

Because it is not possible to distinguish between a caller who is authorized to use the remote access facility of a PBX and the thief who happens to possess an authorization code, all telephone calls originating from the PBX are carried to the terminating number dialed, and the charges

for the completion of the call are passed to the system owner.

The ability of some 800 service providers to supply the originating number of 800 calls may make those customers a less desirable target for remote access fraud because the perpetrator does not enjoy absolute anonymity. However, the sophisticated thief who is attempting to avoid detection may "loop," that is, sequentially dial through a number of different PBXs, and may combine the use of stolen credit cards and other illegal means to frustrate efforts to trace the actual origin of the call. The thief may also use public phone facilities

that likewise cannot be traced back to him.

Take steps to "fraud-proof"

Because the mechanism that permits fraudulent calls to be made is equipment controlled by the customer, neither the long-distance service providers nor the local telcos will take responsibility for the losses resulting from remote access fraud. Consequently, telecommunications managers must take steps to ensure that their systems are secure. **CMA**

Jim Snyder is an Executive Staff Member/Attorney in the Office of Corporate Systems Integrity for MCI Telecommunications.

Guard against PBX fraud

1. Understand all the capabilities of your PBXs and VMBs. The most logical source of information is the vendor who sold or services the equipment. A vendor should be able to describe the fraud-defensive capabilities of a given system.
2. Delete all authorization codes that may have been programmed into the PBX or VMB for testing and service.
3. Frequently audit and change all active codes in a PBX or a VMB. Those no longer authorized - particularly codes which were assigned to former employees, summer interns, and others who are no longer valid users - should be deactivated immediately. Access to authorization codes should always be limited to those who truly have a "need to know."
4. Treat authorization codes just as you would credit card numbers. Each code should be assigned individually, and employees should be instructed as to their confidentiality. For example, they must be told that codes should never be written down on anything which might be discarded, lost or seen by an unauthorized person. Caution them about using pay telephones at airports, hotels, or bus stations: someone may attempt to observe the dialing sequence of the authorization code.
5. Consider replacing the remote access function in the PBX with a virtual private network card which minimizes the company's exposure to fraud. If the remote access function in the PBX is retained, the authorization numbers selected as DISA or RAU codes should be the longest numerical sequence the PBX is designed to handle and choose entirely at random. Because telephone extension numbers, Social Security numbers, and employee identification numbers are easily discovered by thieves, avoid using them as authorization codes.
6. Inform all employees that the person on the other end of a phone conversation may not be the person he or she claims to be. Perhaps a thief, who is trying to learn more about the employee's phone system in order to defraud the company, is posing as a legitimate contact. Remind them that "dumpster divers" regularly scour trash receptacles to obtain discarded company information that may include remote call authorization codes and other proprietary material.
7. Tailor access the PBX to conform strictly with the needs of the company. International and those portions of domestic long distance access that the company does not use should be blocked. If feasible, remote access calling capability should be completely shut down during off-hours and weekends.
8. Establish an unpublished number for the remote access unit/direct inward system access, and program the PBX to wait at least 5 rings before responding to the call.
9. Review billing information to identify unauthorized calling patterns. 800 call detail, a billing option provided by certain 800 service providers, helps identify fraudulent calls to the PBX and/or VMB. Numerous inbound calls of very short duration usually indicate hacking activity, while outbound calls of long duration often, although not always, reflect fraudulent usage. High volumes of calls during off-peak hours (late night and early morning) are also symptoms of possible fraud.
10. Finally, avoid using a steady tone as the prompt to input an authorization code. Instead, use a voice recording or no prompt at all. Whenever an invalid authorization code is entered, the call should either be terminated or routed to a switchboard operator.



MCI

Systems

Integrity

Customer

Support

Program

MCI

**Asst. Director of U.S. Secret Service
(Office of Investigations)**

**Deputy Special Agent in Charge, U.S.S.S.
Special Services Director**

Director, Technical Security, MCI

Director, Information Security, IBM

Deputy Chief Counsel, U.S. Secret Service

Network Development Engineer, MCI

Asst. Director FBI (Intelligence Div.)

Director of Investigations, MCI

Corporate Industrial Hygienist, PEPCO

V.P. Systems Integrity, MCI

Network Systems Planning Engineer, MCI

Chief, Superfund Site Investigations Section, EPA

Director, Federal Systems Div. Security, IBM

Director, Security & Safety,

Special Assistant, U.S. Attorney, U.S. Dept. of Justice

A Wealth of Experience

Members of the MCI Systems Integrity team draw upon key skills and experience derived from a wide variety of previous positions, as well as that gained in advanced training and on the job.

This multi-disciplinary team is built on the experience and skills of systems analysts, engineers, safety officers, security experts and former law enforcement officials, investigators and prosecutors. Operating nationwide, they use every possible means to prevent or minimize a wide range of potential business problems such as telecommunications fraud, information protection, physical security and environmental issues.

As appropriate, the talent, knowledge and experience of the MCI Systems Integrity team is available to support certain customer efforts in these areas. We will share our considerable experience, assist in minimizing fraud, and offer consultative support to help establish or enhance customer programs. Our team is ready to be a part of your team.

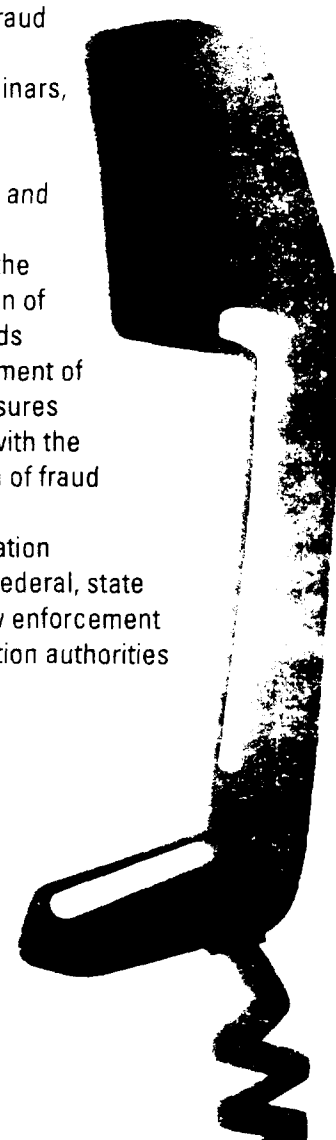




Telecommunication Fraud Prevention

This is a major focus of the MCI Systems Integrity Customer Support program. Efforts are aimed at preventing or reducing the costs of fraud occurring through the abuse of CPE equipment and calling cards.

Steps range from prevention of unauthorized access to identification of fraud perpetrators and include:

- the evaluation, selection and/or recommendation of access control and monitoring equipment and systems
 - development of MCI network-based fraud prevention, detection and control systems
 - increasing fraud awareness through seminars, literature, publicity, consultation and other steps
 - assisting in the determination of fraud methods and development of countermeasures
 - assistance with the identification of fraud perpetrators
 - risk identification
 - liaison with federal, state and local law enforcement and prosecution authorities
- 



Information Security

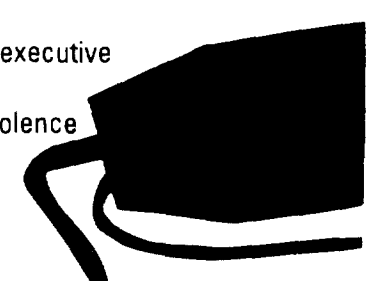
Many of the steps needed for the prevention of telecommunications fraud are also used in information security, particularly security for electronically transmitted or stored information. The Systems Integrity group has expertise in the protection of data, text, voice, image and materials which may be in use, storage or transit that contain proprietary information.

In addition to many of the steps listed under telecommunications fraud, the MCI Systems Integrity group offers experience in these and other areas:

- electronic and physical access controls and monitoring
- computer virus prevention and detection
- disaster recovery
- security organization and planning
- employee, vendor and consultant security issues

Physical Security

The Systems Integrity group also has expertise in the physical security of corporate personnel and property. Certain of these skills may also relate to telecommunications fraud control.

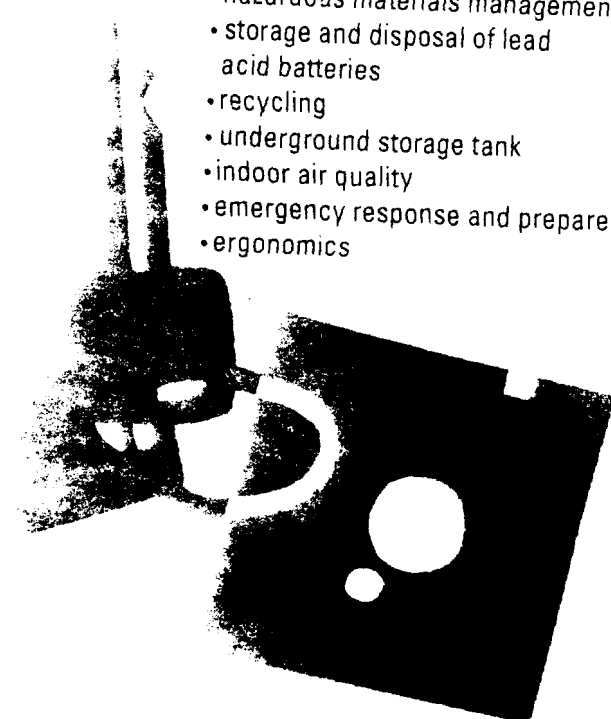
- officers and electronic monitoring systems
 - key control
 - electronic and physical access management
 - crisis management and executive protection
 - threats and/or acts of violence
 - fire and safety training
- 



Environmental Program

MCI has experience in addressing a wide area of environmental compliance issues. Among these are:

- compliance, evaluation, training and awareness program
- hazardous materials management
- storage and disposal of lead acid batteries
- recycling
- underground storage tank
- indoor air quality
- emergency response and preparedness
- ergonomics

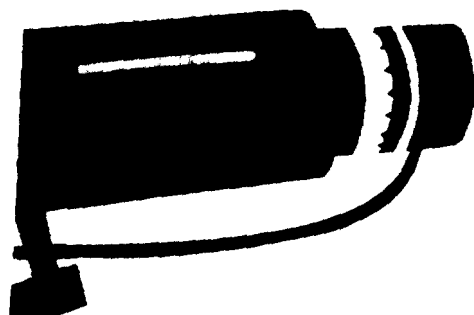


Available Through Your MCI Representative

The services of the MCI Systems Integrity Customer Support Program are available to MCI customers at no cost or on an actual expense basis. They are offered by MCI to supplement and support customer telecommunications fraud control and related programs on a resource as available basis.

Discuss your needs with your MCI Representative. MCI stands ready to work with you.

MCI



In 1988, MCI

highly sophisticated

Systems Integrity Organization

Its mission... to insure that the

telecommunications networks

of MCI and its customers are

as free as possible from un-

authorized access and fraud...

to protect against loss or

damage to corporate information

and records... to maintain the

physical security of our

equipment and personnel

and compliance with

regulatory and safety



have been put in place. They will also enable out-dialing features that do not normally exist on the PBX. These situations can be difficult to detect. Hackers have been known to change the system at 8:00 pm to allow fraud calls. Then, at 3:00 am the next morning, they re-program the system back to its original configuration. A telecom manager who reviews the configuration in the morning will not be looking at the configuration that was abused. This can lead to delays in resolving the abuse.

FRAUD SOLUTION(S):

To solve this problem a Security Access Unit (SAU) should be placed in front of the maintenance port. SAUs provide another level of user ID and password protection. This ID and password should be controlled by the PBX owner and not any vendor. In addition, SAUs can be set up to further validate a user via callback or various token devices. While somewhat expensive, there are products which use voice validation for authentication.

LOOPING

FRAUD METHOD(s):

Looping is a method which call sell operators use to circumvent restrictions that IXCs put in the networks to control calling card fraud. Looping is also used to avoid identification of the origination of the calls. As an example, all carriers block calling card calls bound for the Dominican Republic that originate in NYC. If a call-sell operator is able to obtain a dial tone from a PBX but is not able to dial 809 or 011 call directly, they will revert to looping. They could dial an 800 number outbound from the PBX. The 800 number could be to another PBX or could be a calling card or operator access number. They could also dial 950 carrier access numbers. Lastly, they can dial various 10XXX carrier access codes. In any case they can still use the PBX to place a fraud call. If the PBX is not in NYC they can use the calling card. Use of the 10XXX codes could allow for direct billing to the PBX.

FRAUD SOLUTION(s):

Many times a PBX owner will also take proactive actions to minimize the risk of fraud. These actions include:

- Blocking of 011 or 809 dialing.
- Block 10XXX codes if possible.
- Block 950 access if possible.
- Monitor 10XXX, 950 and 800 calling on the system to identify possible looping.

Typical PBX Fraud Methods and Summary Solutions

M C I S y s t e m s I n t e g r i t y

The **MCI Network** *Means* **BUSINESS**

MCI

COMNET '93

DISA

FRAUD METHOD(s):

DISA is designed to allow remote access to a PBX and then originate an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call-sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer." The "war dialer" dials telephone numbers randomly, generally 800 numbers, until a modem or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (auth codes). Codes are "frequently" but not always distributed to pirated voice mail systems and computer bulletin boards. The codes are usually distributed to a network of call-sell operators and may also be posted on bulletin boards and voice mail systems.

FRAUD SOLUTIONS(s):

There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin, auth codes should be made as long as possible. At very least a factor of 10,000 should exist between the active codes. For example, if there are 10 users the code should be at least 5 digits long ($10 \times 10,000 = 100,000$ or 5 digits). Auth codes should be randomly scattered throughout the possible range but not easily defined (i.e. 1234 or 1111). Class of service restrictions should be applied to the auth codes. Only users with a truly legitimate need should be allowed International dialing through the DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show the number of times and minutes an auth code is used in a day. If possible, the dollar value of those calls should also be noted on the reports.

VOICE MAIL BOXES (VMB)

FRAUD METHOD(s):

There are two types of VMB Systems fraud. The first type occurs when a hacker takes over a box and uses it to communicate with other hackers. This can be expensive if access is gained to the VMB System via an 800 number. In this situation, a hacker typically hacks out the box password and changes it along with the greeting.

FRAUD SOLUTIONS(s):

To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the phone. If a telecom person can add, delete and change boxes via the phone, so can a hacker.
- Do not have active mailboxes that do not have an owner.
- Passwords should be at least 6 digits long.
- If possible, passwords should expire every 30-90 days.

VOICE MAIL BOXES (VMB)

FRAUD METHOD(s)

The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a phone on the system. If the PBX is not set up properly the transfer can be made directly to dial tone. In other instances the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the tie line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBXs have Trunk Access Codes (TACs) or Facility Access Codes (FACs). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TACs or FACs.

FRAUD SOLUTION(s):

Steps to prevent this type of fraud include:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4 digit extension, if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

CALL ATTENDANT

FRAUD METHOD(s):

Call attendants are used by many companies to replace a switchboard operator. When a call attendant answers, the caller is generally given numerous options. A typical greeting would be, "Hello, you've reached ABC Bank. Please enter (1) for Auto Loans, (2) for Home Mortgages. If you know the number of the person you are calling please enter that now." In many call attendants, option nine would be allowed on outbound calls. In addition, when asked to enter an extension the call-sell operator will enter 9180 or 9011. If the system is not properly configured, the call attendant will pass the call back to the PBX. The PBX will react to the 9 as a request for a dial tone. The 180 would become the first numbers of a 1-800 call to the Dominican Republic. The 011 would be treated as the first digits of an International call.

FRAUD SOLUTION(s):

- Ensure muted features are disabled. In the above example the caller has been offered options 1 and 2. The other options have been muted. They must be shut off to guarantee that the muted features are not active and can not be accessed.
- Allow only line side access to any calls passed by the call attendant to the PBX.
- Disallow TAC and FAC access to the call attendant trunks.
- Configure the call attendant so that only valid extensions are transferred back to the PBX.

MAINTENANCE PORTS

FRAUD METHOD(s):

Maintenance ports are the most recent type of abuse. In this scenario a hacker finds a maintenance port number with his "war dialer." He/she then hack out the user ID and password. At this point they have access to all the features and controls within the PBX. They will program out any restrictions that

Using Your Vnet Card Is As Easy As 1-2-3 . . .

When calling from the U.S. and Canada:

1. Dial 1-800-950-1111.

2. When you hear the first tone,

Dial 0 + area code + number; or

**Dial 01 + country code + city code + number
(for international calls); or**

**Dial 0 + seven-digit private dialing plan
number (if used by your company).**

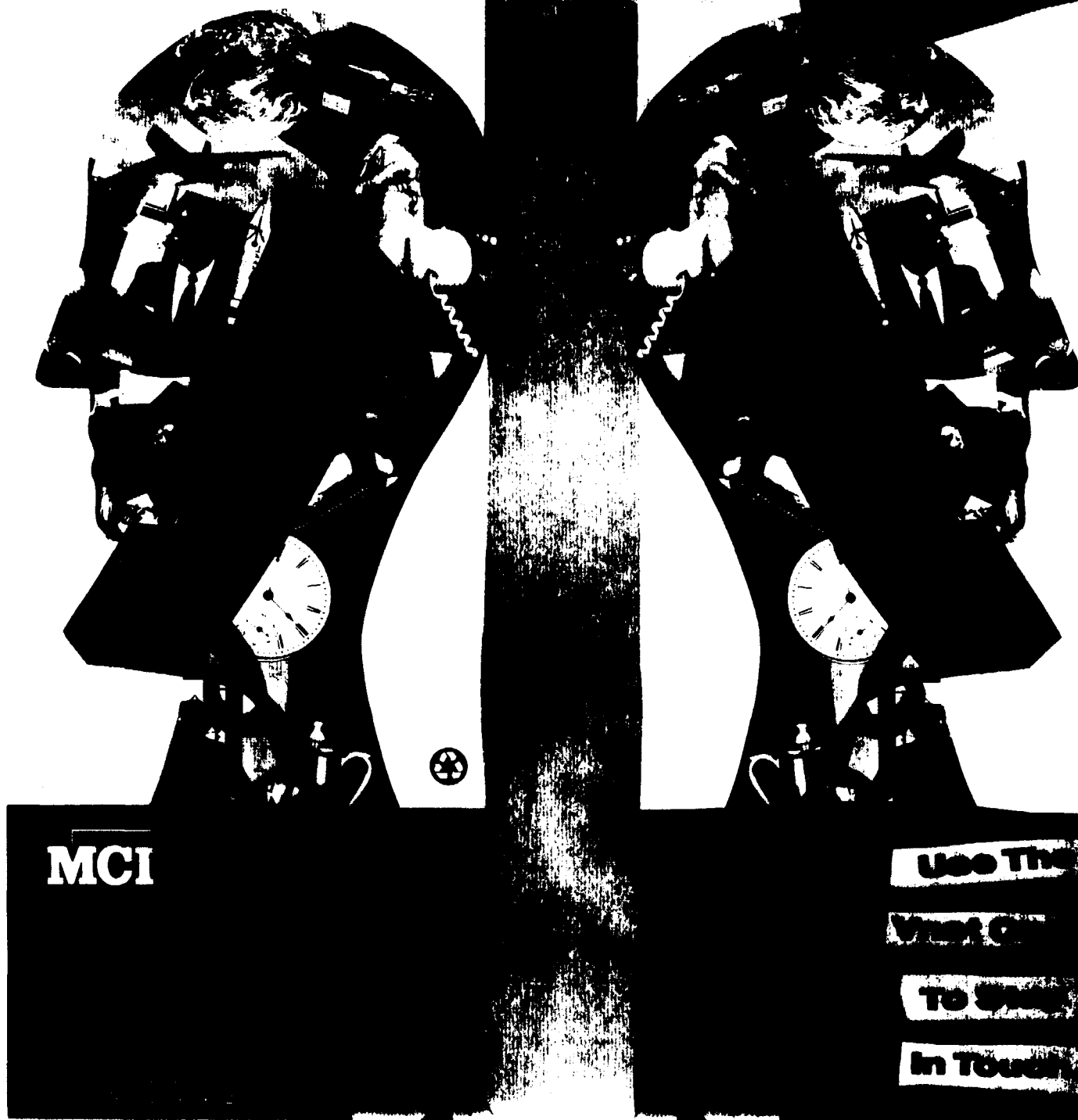
3. When you hear the second tone,

**Dial your authorization code (the number
on the front of your Vnet Card).**

To make additional calls, you don't have to start over with your access number—simply press the # sign for a full second instead of hanging up, and then repeat step 2. (You don't even have to dial the authorization code again!)

If you dial a wrong number, press the # sign for a full second, then dial the correct number. If it is the first call, dial the authorization code at the second tone. If not, there's no need to redial the authorization number.

- If you are calling from a rotary phone, dial the access number and wait for an operator to assist you.
- If you are calling from a payphone, please check the instructions on the payphone for making an "800" call; you may need to dial 0 800-950-1111.
- If you are calling from a hotel phone, use the hotel's instructions for making an "800" call, dial 1-800-950-1111 and follow steps 2 and 3 to complete the call. (You may still be billed a surcharge by the hotel.)



■ **One number is all you need**—from either a touch-tone or rotary phone. When you're traveling, convenience and efficiency are critical. When it comes time to make a call, you don't have time to look up a lot of numbers.

■ **All the benefits of your company's phone network—when you're on the road!** If your company has a seven-digit private dialing plan, the same number you use to call your colleagues from your office can be used with the Vnet CardSM. You also get the benefit of other network services, such as having your call automatically forwarded, or receiving special "help messages" when there's any kind of change or problem.

Or More Convenient . . .

■ **Once you access the system, you can make as many calls as you want.** When your conversation is finished, instead of hanging up, simply press the # key and you can place another long distance call.

■ **It's also easy to call from an ever-expanding list of other countries**—all instructions are contained in the wallet-sized, easy-to-follow Vnet Card Global ReachSM Pocket Guide.

Or More Practical.

■ **The Vnet Card offers your company considerable cost savings.** Every call you make using the Vnet Card contributes to your company's savings plan with MCI[®]—the more you use it, the more your company will save! When you use your Vnet Card to call your office or any of your company's major facilities, you save even more because you'll be going through your company's private network. The Vnet Card's fast connections will save you time too!

If you have a problem with your Vnet Card . . . Call customer service to report the problem (the number is written on the carrier in which you received your Vnet Card). For your convenience, you can write this number in the space provided on the back of your card.

If your card is lost or stolen . . . You should immediately call the customer service number.

If you dial a wrong number . . . You can receive immediate credit. Simply dial 1-800-950-1111, wait for the operator, and explain that you want credit.

If you get a recording that says you are not authorized to call the number you dialed . . . See your manager. To increase security in case of a lost or stolen Vnet Card, your company can specify calling privileges for each card. The area covered is determined by where you do business. If you need to make calls outside of the area set for your card, your manager can make the changes to permit such calls.

If you need to make calls from outside the U.S. or Canada . . . Instructions for using your Vnet Card are provided in your Vnet Card Global Reach Pocket Guide, which you received with your card. MCI is continuously adding countries in which you can use your Vnet Card. Before your next business trip abroad, call 1-800-444-4141 to get the most recent list of countries and the free-phone (toll-free) numbers for each one.

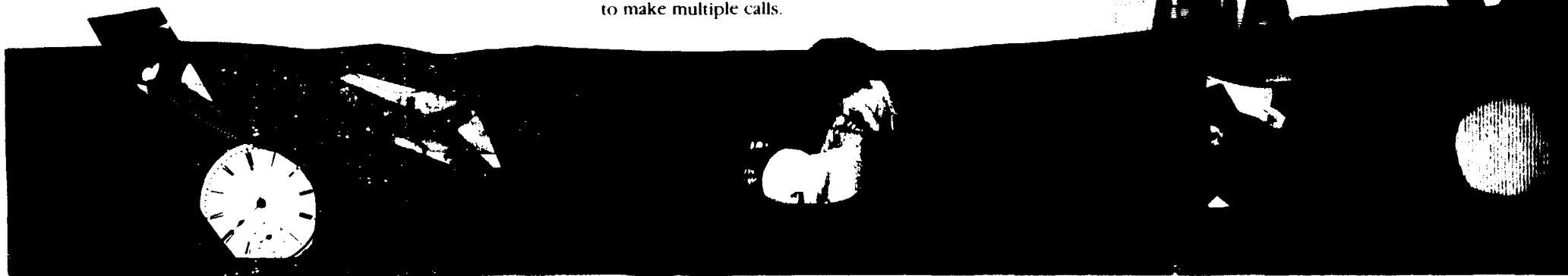
If you are trying to access Vnet[®] from any phone in the U.S. . . . Dial the "800" access number for all types of calls from all types of phones. (Other companies require several different access numbers depending on the type of call and the pay-phone carrier.) This access number allows you to make multiple calls.

Use Your Vnet Card With Care

Your Vnet Card can help you and your company fight the fraudulent use of credit cards by programming your card to cover only those areas where you actually do business. Should your card be lost or stolen, the risk of fraud is significantly reduced because your Vnet Card will only operate within designated areas.

Here are some other ways you can help combat fraud:

- **If your Vnet Card is lost or stolen,** report it to customer service (the number written on the Vnet Card carrier) as soon as you become aware of it.
- **Don't share your Vnet Card with other people**—protect it as you would any credit card.
- **Try to memorize your Vnet Card authorization code** (the number on the front of the card). The less you take it out in public, the less likely it is that someone will steal it or copy down the number.
- **Be aware of people loitering around payphones.** If you have not memorized your number, try to prevent others from seeing your Vnet Card when you take it out to use it.
- **When placing operator-assisted calls, speak directly into the phone in a normal tone of voice**—be careful not to allow anyone to hear your authorization number.



For more information

The National Fraud Information Center provides information to consumers about current telephone frauds and tips for avoiding fraud. Center staff is available from 10:00 a.m. to 4:00 p.m. to answer questions, provide information and names and addresses of agencies and organizations that offer assistance to consumers. Recorded information is available 24 hours a day. Calls requiring personal assistance, when received after hours, will be returned as soon as possible.

National Fraud Information Center

Consumer Assistance 1-800-876-7060

TDD 202-737-5084

This brochure was produced on behalf of the National Fraud Information Center by MCI Consumer Markets and MCI Systems Integrity.

**NATIONAL
FRAUD**
INFORMATION CENTER

MCI

AVOIDING PHONE FRAUD

A MESSAGE FROM MCI

P H O N E F R A U D

NEW TECHNOLOGY, OLD SCAMS

The telephone offers American consumers an inexpensive, efficient way to communicate directly with family, friends and businesses. New telephone technologies, from increasingly versatile 800 and 900 number services to fax machines and cellular telephones, have changed the way we communicate with each other.

To use calling cards or 800 and 900 numbers, callers do not have to understand the technologies and databases that make these kinds of services possible. Following a few simple steps, callers learn quickly to complete these calls with a minimum of effort.

Unfortunately, con artists have learned to use the telephone to promote confusion and deceive consumers. Using the communications tools of legitimate businesses, they sell everything from fraudulent investments, loans and travel bargains to boats that turn out to be inflatable rafts. Like burglars stealing through the night, they use telephones to become "invisible".

American consumers can outsmart the telephone scam artists. By following some rules for telephone shopping, callers can make sure that they don't give a criminal a chance.

OBSERVE A FEW BASIC PRECAUTIONS WHEN MAKING PURCHASES BY TELEPHONE

Telephone shopping is so popular with Americans that con artists recognized an opportunity to deceive consumers. They could sell their valueless products or phony securities while hiding behind the anonymity of the

telephone. These con artists started out by simply calling consumers and pressing them into buying their worthless wares. After this approach stopped working, they often used newspaper and cable advertising, postcards and other types of mail to urge their "unsuspecting prospects" to call them. Their techniques are sometimes a near-perfect imitation of the techniques of legitimate businesses.



"I was really excited—I received a postcard in the mail telling me I'd won a free prize if I called a certain number. I ended up sending the company money for some merchandise, and never received anything."

AVOID FRAUD — FOLLOW THESE SIMPLE PROTECTIVE MEASURES

- 1. Make sure that you know the company with which you are dealing, whether the company calls you or you make the call.** The company should be willing to provide its name, address and phone number.
- 2. If you need more information about a company,** check it out with the consumer protection office or the office of the attorney general where the business is located.
- 3. Do not give credit card or checking account information over the telephone unless you know the company and are making a purchase.**
- 4. Ask for written information about sales transactions.** You should expect to receive a written confirmation of costs, and terms and conditions of purchase transactions. Ask about price, including all fees, delivery charges, sales tax. Insist on a detailed description of the goods and services that you are considering for purchase.
- 5. Ask about guarantees and refunds, and make sure you have them in writing before you make a financial commitment.**
- 6. Do not agree to send cash by mail.**
- 7. Resist high-pressure tactics.**
- 8. Be skeptical of offers that sound too good to be true.**

USING A CALLING CARD

Thieves do not need the calling card itself to use it for fraudulent purposes. They need only to learn the 14 digit authorization code to "steal" your card from you. Important do's and don'ts include:

- 1. Do memorize your calling card number.** Memorization of your card number reduces the risk of the number being stolen as you use the card.
- 2. Do be aware of people loitering around the phone.** People may pretend to be having a conversation on a nearby payphone, to place themselves in a good position

to copy down your authorization code while you are making your call. Stand directly in front of the phone while pressing the authorization code numbers. Also, use a normal conversational tone when reciting the number to an operator.

- 3. Don't give your calling card number to telephone security or others.** Any legitimate telephone representatives already have your authorization code and will not need to ask you for it.
- 4. Don't share your calling card number with others.** Your calling card number can be abused just like any credit card; guard the number as you would a Visa or MasterCard number.
- 5. Do report lost or stolen cards.** Report the loss to the appropriate long distance company as soon as possible to minimize the risk of abuse by thieves.

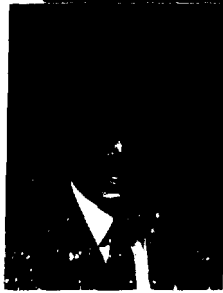
DON'T ACCEPT THIRD-PARTY CALLS FROM PEOPLE YOU DON'T KNOW

Third-party calls are calls billed to your telephone, by someone calling outside your home or office. Operators, before placing third-party calls, must obtain permission from the party who will be billed for the call. It is appropriate to approve such calls when you know the person calling, and wish to pay for the call. Do not give permission to unknown parties to bill calls to your number.

900 NUMBERS: CONSUMER SAFEGUARDS IN PLACE

Many companies and organizations provide information about their products or services, take orders, or offer advice or educational messages via 900

"What happens when I call a 900



"Someone charged calls on my calling card number. How can that happen when the calling card was never out of my wallet?"

long distance service. Most businesses charge consumers who use their 900 number lines. Federal rules and long distance company regulations require providers of 900 service to protect consumers by preceding the billable part of the call with a statement, or preamble, explaining:

- 1. The cost of the call per-minute or the flat rate, if it will exceed \$2.00.** The name of the information provider and a description of the information or service to be provided must be clearly indicated.
- 2. The exact point when billing will begin (for example, a beep tone might show when the charges start for the call).** The program must allow you to disconnect before that point without charge.
- 3. If the program is directed toward minors, it must warn them that they must obtain parental permission to complete the call.**

Federal rules require long distance carriers to provide the name, address and customer service telephone number of the information provider, at no charge. Local telephone companies must offer a free (for the first request) 900 service block option to residential customers. Local phone companies may not disconnect local phone service for non-payment of interstate 900 pay-per-calls.

In addition, to further protect consumers, long distance carriers impose additional restrictions on the types of 900 programs for which they will perform the billing and collection.

USING 800 NUMBERS

When 800 service was first introduced, it was widely advertised as toll-free. The intent of the long distance carriers is to continue to promote and protect toll-free 800 service. In some short-lived scams, con artists distorted the 800 service by confusing consumers and charging for calls that they expected would be free.

To protect callers, long distance carriers prohibit charging callers for information carried on 800 numbers unless the caller has an established billing relationship with the 800 information service or uses a credit card to pay for the service. For example, a caller could dial an 800 number to reach a stock information service which charges a fee, but would be required to have a billing relationship with the service or use a credit card to receive the service. The 800 information service **CANNOT** bill the customer's phone number or permit charges by a third party with whom the consumer has no business relationship.

If you call an 800 number and are asked to call another long distance number or to receive a collect call to obtain additional information, you may be charged for the collect or additional call. The collect or additional call is not a part of the original 800 call.



number? When do the charges begin?"



**TYPICAL PBX FRAUD METHODS
AND
SUMMARY SOLUTIONS**

MCI

SYSTEMS INTEGRITY

OUTLINE

- DISA
- VOICE MAIL BOXES(VMB)
- CALL ATTENDANT
- MAINTENANCE PORTS
- LOOPING

(Continued)

VOICE MAIL BOXES (VMB)

FRAUD METHOD(s)

The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a telephone on the system. If the PBX is not set up properly the transfer can be made directly to dialtone. In other instances, the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBX have Trunk Access Codes (TAC's) or Facility Access Codes (FAC's). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TAC's or FAC's.

FRAUD SOLUTION(s):

Steps to prevent this type of fraud include:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4 digit extensions, if transferring is allowed.
- Blocking 8 & 9 access (8& 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

CALL ATTENDANT

FRAUD METHOD(s):

Call attendants are used by many companies to replace a switchboard operator. When a call attendant answers, the caller is generally given numerous options. A typical greeting would be, "Hello, you've reached Nations Bank, please enter one for Auto Loans, two for Home Mortgages. If you know the extension of the person you are calling, please enter it now." In many call attendants, option nine would be allowed on outbound calls. In addition, when asked to enter an extension the call sell operator will enter 9180 or 9011. If the system is not properly configured the call attendant will pass the call back to the PBX. The PBX will react to the 9 as a request for a dial tone. The 180 would become the first numbers of a 1-809, call the Dominican Republic. The 011 would be treated as the first digits of an International call.

FRAUD SOLUTION(s):

- Ensure muted features are disabled. In the above example the caller has been offered options 1 and 2. The other options have been muted. They must be shut off to guarantee that the muted features are not active and cannot be accessed.
- Allow only line side access to any calls passed by the call attendant to the PBX.
- Disallow TAC and FAC access to the call attendant trunks.
- Configure the call attendant so only valid extensions are transferred back to the PBX